Jul-22-21

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

CYBER WEEKLY AWARENESS REPORT

July 22, 2021

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

Internet Storm Center Infocon Status

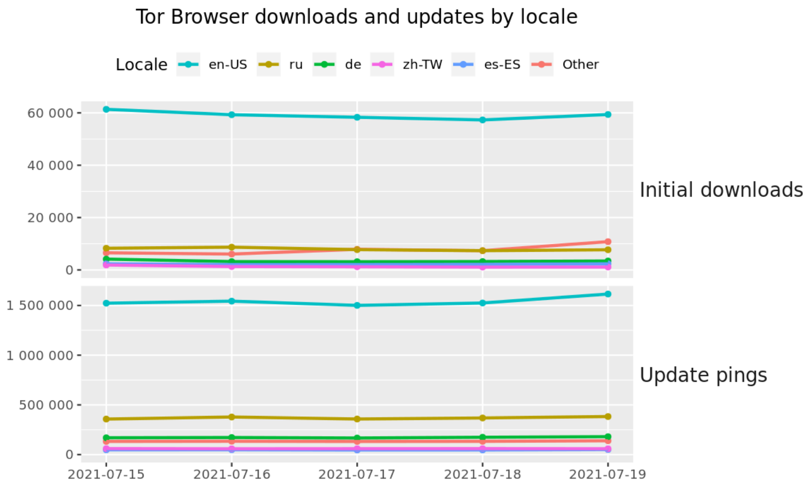
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.

Just released!!! Web App Hacking: Carnage & Pwnage



The Tor Project - https://metrics.torproject.org/

Interesting News

* Subscribe to this OSINT resource to recieve it in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* NSO Will No Longer Talk To The Press About Damning Reports
* Long-Awaited Bill Would Force Breach Victims To Contact CISA
* 740 Ransomware Victims Named On Data Leak Sites In Q2 2021
* Saudi Aramco Denies Breach After Hackers Hawk Stolen Files
* NPM Package Steals Passwords Via Chrome's Account Recovery Tool
* Home And Office Routers Come Under Attack By China State Actors, France Warns
* Researchers Hid Malware Inside An AI's Neurons And It Worked Scarily Well
* Fortinet's Security Appliances Hit By Remote Code Exec Vuln
* EU Plans To Make Bitcoin Transfers More Traceable
* MacOS Being Picked Apart By $49 XLoader Data Stealer
* Why Apple's Walled Garden Is No Match For Pegasus Spyware
* TSA Announces New Pipeline Security Order
* Hundreds Of Touchscreen Ticket Machines Hit By Ransomware Attack
* China Denies Being Behind Major Microsoft Hack
* Apple Under Pressure Over iPhone Security After NSO Spyware Claims
* Chinese Hackers Hid Hacked Data In A Donald Trump Picture
* HP Patches Vulnerable Driver Lurking In Printers For 16 Years
* Hackers Got Past Windows Hello By Tricking A Webcam
* Swedish Man Sentenced For Gold-Backed Cryptocurrency Scam
* UK And White House Blame China For Microsoft Exchange Server Hack
* Facebook Catches Iranian Spies Catfishing US Military Targets
* U.S. Gov't Offers $10 Million For Info On Hackers Targeting Infrastructure
* Chinese APT LuminousMoth Abuses Zoom Brand For Gov't Attacks
* Hooking Candiru: Another Mercenary Spyware Comes Into Focus
* Microsoft: New Unpatched Bug In Windows Print Spooler

Krebs on Security

Unfortunately, at the time of this report, the Krebs resource was not availible.

LATEST NEWS

Dark Reading

* 7 Hot Cyber Threat Trends to Expect at Black Hat
* Law Firm for Ford, Pfizer, Exxon Discloses Ransomware Attack
* US Accuses China of Using Criminal Hackers in Cyber Espionage Operations
* How Gaming Attack Data Aids Defenders Across Industries
* NSO Group Spyware Used On Journalists & Activists Worldwide
* When Ransomware Comes to (Your) Town
* 7 Ways AI and ML Are Helping and Hurting Cybersecurity
* Breaking Down the Threat of Going All-In With Microsoft Security
* Researchers Create New Approach to Detect Brand Impersonation
* Recent Attacks Lead to Renewed Calls for Banning Ransom Payments
* 4 Future Integrated Circuit Threats to Watch
* How to Attract More Computer Science Grads to the Cybersecurity Field
* Attackers Exploited 4 Zero-Day Flaws in Chrome, Safari & IE
* State Dept. to Pay Up to $10M for Information on Foreign Cyberattacks
* CISA Launches New Website to Aid Ransomware Defenders
* Microsoft: Israeli Firm's Tools Used to Target Activists, Dissidents
* IoT-Specific Malware Infections Jumped 700% Amid Pandemic
* How to Bridge On-Premises and Cloud Identity
* What to Look for in an Effective Threat Hunter
* SonicWall: 'Imminent' Ransomware Attack Targets Older Products

The Hacker News

* APT Hackers Distributed Android Trojan via Syrian e-Government Portal
* Reduce End-User Password Change Frustrations
* Oracle Warns of Critical Remotely Exploitable Weblogic Server Flaws
* Another Hacker Arrested for 2020 Twitter Hack and Massive Bitcoin Scam
* Malicious NPM Package Caught Stealing Users' Saved Passwords From Browsers
* XLoader Windows InfoStealer Malware Now Upgraded to Attack macOS Systems
* Several New Critical Flaws Affect CODESYS Industrial Automation Software
* [eBook] A Guide to Stress-Free Cybersecurity for Lean IT Security Teams
* New Windows and Linux Flaws Give Attackers Highest System Privileges
* 16-Year-Old Security Bug Affects Millions of HP, Samsung, Xerox Printers
* This New Malware Hides Itself Among Windows Defender Exclusions to Evade Detection
* US and Global Allies Accuse China of Massive Microsoft Exchange Attack
* Researchers Warn of Linux Cryptojacking Attackers Operating from Romania
* Turns Out That Low-Risk iOS Wi-Fi Naming Bug Can Hack iPhones Remotely
* Five Critical Password Security Rules Your Employees Are Ignoring

LATEST NEWS

Security Week

* Atlassian Patches Critical Vulnerability in Jira Data Center Products
* Google Cloud Unveils New SOC, IDS Solutions
* China-Linked APT31 Abuses Hacked Routers in Attacks, France Warns
* iOS Security Update Patches Recently Disclosed Wi-Fi Vulnerability
* CISA Details Malware Used in Attacks Targeting Pulse Secure Devices
* Is Your SecOps Solution Keeping Up?
* Dell Patches Critical Vulnerabilities in OpenManage Enterprise
* UK Man Arrested in Spain, Charged in US With Twitter Hack
* Biden to Meet Next Month With Private Sector on Cyber Issues
* Google Cloud Introduces New Zero Trust Offerings for Government
* Saudi Aramco Facing $50M Cyber Extortion Over Leaked Data
* Ransomware Attack on UK Rail System - Spray and Pray or Targeted?
* Microsoft Acquires Cloud Security Start-up CloudKnox
* DNSFilter Raises $30 Million in Series A Funding
* Industrial Firms Warned of Risk Posed by Cloud-Based ICS Management Systems
* Oracle Releases July 2021 CPU With 342 Security Patches
* Chrome 92 Brings Several Privacy, Security Improvements
* Macron Among 14 Heads of States on Potential Spyware List
* Millions of Devices Affected by Vulnerability in HP, Samsung, Xerox Printer Drivers
* Zero Trust, We Must
* Adobe Patches 21 Vulnerabilities Across Seven Products
* Fortinet Patches Remote Code Execution Vulnerability in FortiManager, FortiAnalyzer
* Google Enhances Protections in Cloud Armor Web Security Service
* Russian Hacker Levashov Sentenced to Time Already Served

Infosecurity Magazine

Unfortunately, at the time of this report, the Infosecuroty Magazine resource was not availible.

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Microsoft Takes Down Homoglyph Domains
* [HEADS UP] 2021 Tokyo Olympics Mean Olympic-Themed Phishing Attacks
* Mint Mobile, Porting Numbers, and Identity Theft
* Microsoft Continues to be the Top Impersonated Brand in Phishing Attacks
* The Cost and Impact of Cybercrime Can Now Be Measured in a Single Minute
* CyberheistNews Vol 11 #28 [HEADS UP] Live Phishing Attack Uses New Infection Technique to Deliver Mal
* [INFOGRAPHIC] New Report Shows Users Are Falling for Security and HR-Related Phishing Attacks
* New LuminousMoth APT Takes a Double-Infection Vector Approach to Attacks
* Nearly Every Organization Has Had an Insider-Caused Data Breach in the Last Year
* Facebook Disrupts Iranian Social Engineering Operation

ISC2.org Blog

* The Role of Culture in Compliance
* Malware, Cybercrime and Cloud Security
* Cybersecurity Professionals to Newcomers: Focus on Vendor-Neutral Certifications
* Be The Strongest Link In Your Organization's Supply Chain
* Trending: 4,500+ Cyber Pros Enroll in Free (ISC)2 Ransomware Course in Less Than a Month in Order to

HackRead

* WifiDemon - iPhone Wifi bug exposed devices to remote attacks
* Israeli spyware used in hacking phones of activists, journalists globally
* Misconfigured AWS bucket exposed 421GB of Artwork Archive data
* Google issues patches for Chrome flaw for Windows, Mac and Linux
* SolarWinds hackers exploited iOS 0-day to compromise iPhones
* New LinkedIn phishing campaign found using Google Forms
* A brief guide on building audio and video live streaming platform

Koddos

* WifiDemon - iPhone Wifi bug exposed devices to remote attacks
* Israeli spyware used in hacking phones of activists, journalists globally
* Misconfigured AWS bucket exposed 421GB of Artwork Archive data
* Google issues patches for Chrome flaw for Windows, Mac and Linux
* SolarWinds hackers exploited iOS 0-day to compromise iPhones
* New LinkedIn phishing campaign found using Google Forms
* A brief guide on building audio and video live streaming platform

LATEST NEWS

Naked Security

* S3 Ep42: Viruses, Nightmares, patches, rewards and scammers [Podcast]
* Windows "HiveNightmare" bug could leak passwords - here's what to do!
* Apple iPhone patches are out - no news if recent Wi-Fi bug is fixed
* S3 Ep41: Crashing iPhones, PrintNightmares, and Code Red memories [Podcast]
* More PrintNightmare: "We TOLD you not to turn the Print Spooler back on!"
* Want to earn $10 million? Snitch on a cybercrook!
* The Code Red worm 20 years on - what have we learned?
* Home delivery scams get smarter - don't get caught out
* Don't get tricked by this crashtastic iPhone Wi-Fi hack!
* Where do all those cybercrime payments go?

Threat Post

* Industrial Networks Exposed Through Cloud-Based Operational Tech
* Apple Issues Urgent iPhone Updates; None for Pegasus Zero-Day
* Microsoft Issues Windows 10 Workaround Fix for 'SeriousSAM' Bug
* NPM Package Steals Passwords via Chrome's Account-Recovery Tool
* Indictments, Attribution Unlikely to Deter Chinese Hacking, Researchers Say
* Kubernetes Cloud Clusters Face Cyberattacks via Argo Workflows
* French Launch NSO Probe After Macron Believed Spyware Target
* Tracking Malware and Ransomware Domains in 2021
* MacOS Being Picked Apart by $49 XLoader Data Stealer
* Researchers: NSO Group's Pegasus Spyware Should Spark Bans, Apple Accountability

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

LATEST NEWS

IBM Security Intelligence

* This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered
* Beyond Ransomware: Four Threats Facing Companies Today
* How to Fix the Big Problems With Two-Factor and Multifactor Authentication
* Avoid Blind Spots: Is Your Incident Response Team Cloud Ready?
* How Data Discovery and Zero Trust Can Help Defend Against a Data Breach
* Two (or More) Is Better Than One: Digital Twin Tech for Cybersecurity
* FragAttacks: Everything You Need to Know
* 3 Myths About Threat Actors and Password Safety
* Cyber Insurers Might Be Making the Ransomware Problem Worse
* When 'Later' Never Comes: Putting Small Business Cybersecurity First

InfoWorld

* "Do More with R" video tutorials
* How to run R in Visual Studio Code
* An introduction to time series forecasting
* What is SaaS? Software as a service defined
* Java state API would speed app startup
* Get your Visual Studio extensions ready for 64-bit
* 6 essential Python tools for data science-now improved
* Visual Studio Code 1.58 improves debugging, Jupyter Notebook support
* Why companies get stuck in the middle of their devops journey
* How to use HTTP logging in ASP.NET Core 6

C4ISRNET - Media for the Intelligence Age Military

* Submarine leaders want to tap into JADC2 network without giving away their position
* To afford next-gen combat aircraft, the US Air Force will make cuts to ISR inventory
* National Reconnaissance Office wants a more distributed architecture
* Path for DARPA tech to become part of military's JADC2 enterprise still unclear
* Planning for a rainy day in space: How America can build a resilient space future
* US Army matures tactical tools for trustworthy data, cyber op action plans
* In a couple years, soldiers in Strykers can learn enemy locations before exiting the vehicles
* US military must avoid a 'Kasserine Pass' failure for space power
* 'There are so few people that get this': Biden faces hurdle in finding new pick for Pentagon's top bu
* Biden to nominate defense industry expert Andrew Hunter as Air Force acquisition boss

The Hacker Corner

Conferences

* Marketing For Cybersecurity
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* An EPYC escape: Case-study of a KVM breakout
* Fuzzing iOS code on macOS at native speed

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* HTB Business CTF 2021
* ImaginaryCTF 2021
* IJCTF 2021
* CyBRICS CTF 2021
* Crypto CTF 2021
* UIUCTF 2021
* RTLxHA CTF 21
* RaRCTF 2021
* TSG CTF 2021
* BSides Noida CTF

VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* HackathonCTF: 2
* Hackable: II
* VulnCMS: 1
* hacksudo: ProximaCentauri
* Tech_Supp0rt: 1

Tools & Techniques

Packet Storm Security Tools Links

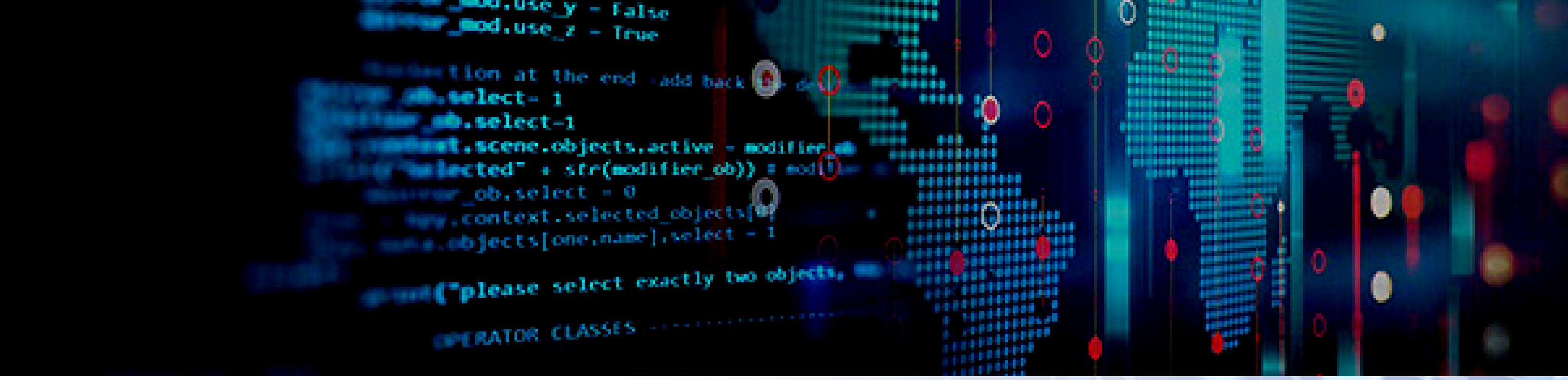
* Lynis Auditing Tool 3.0.6
* American Fuzzy Lop plus plus 3.14c
* Hashcat Advanced Password Recovery 6.2.3 Source Code
* Hashcat Advanced Password Recovery 6.2.3 Binary Release
* Wireshark Analyzer 3.4.7
* UFONet 1.7
* Global Socket 1.4.33
* Zeek 4.0.3
* Stegano 0.9.9
* SQLMAP - Automatic SQL Injection Tool 1.5.7

Kali Linux Tutorials

* DNSrr : A Tool Written In Bash, Used To Enumerate All The Juicy Stuff From DNS
* Whisker : A C# Tool For Taking Over Active Directory User And Computer Accounts By Manipulating Their
* The-Bastion : Authentication, Authorization, Traceability And Auditability For SSH Accesses
* DNSStager : Hide Your Payload In DNS
* Bughound : Static Code Analysis Tool Based On Elastic search
* Kali-Whoami : A Privacy Tool Developed To Keep You Anonymous On Kali Linux At The Highest Level
* Exploit_Mitigations : Knowledge Base Of Exploit Mitigations Available Across Numerous Operating Syste
* Ventoy : A New Bootable USB Solution
* Redteam-Hardware-Toolkit : Red Team Hardware Toolkit
* Injector : Complete Arsenal Of Memory Injection And Other Techniques For Red-Teaming In Windows

GBHackers Analysis

* Critical Oracle Weblogic Flaw Let Remote Attacker Take Control of The System
* Millions of Printers Worldwide Vulnerable To The 16-Year-Old Bug
* Russian APT Hackers Launched A Mass Global Brute Force Attack to Hack Enterprise & Cloud Networks
* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices
* 5 Key Phases of Ethical Hacking



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Getting started in DFIR: Testing 1,2,3
* DFIR Summit 2021
* STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign
* FOR585: Smartphone Forensic Analysis In-Depth

Defcon Conference

* DEF CON China Party 2021 - Keynote Interview Excerpt - Steve Wozniak, The Dark Tangent
* DEF CON China Party 2021 - Whispers Among the Stars - James Pavur
* DEF CON China Party 2021- Wall of Sheep: Hilarious Fails and the Sheep Behind Them - Riverside
* DEF CON China Party - Cooper Quintin- Detecting Fake 4G Base Stations in Real Time

Hak5

* HakByte: Use Android Studio to Learn Android App Security Part 3
* A Look at Glytch's Pocket Hardware Hacking Kit
* HakByte: Use Android Studio to Learn Android App Security Part 2

The PC Security Channel [TPSC]

* Discord Ransomware
* Windows 11: Better Security?

Eli the Computer Guy

* eBeggar Wednesday - ALPHA MALE Edition
* "Easy" Computer Speech Recognition with Azure Cognitive Services and Python
* How to Become a YouTuber
* How to Become a Tech Professional

Security Now

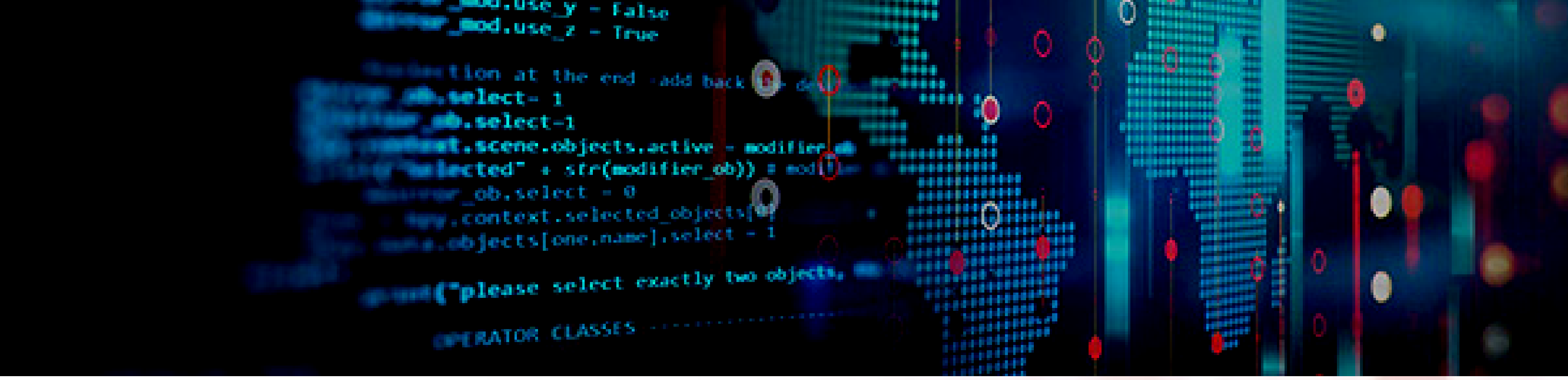
* REvil Vanishes! - Chrome Zero-Day Vulnerability, iOS WiFi SSID Bug, Patch Tuesday Review
* REvil's Clever Crypto - Microsoft Fails to Patch PrintNightmare & Sodinokibi Malware's Crypto Design

Troy Hunt

* Weekly Update 252

Intel Techniques: The Privacy, Security, & OSINT Show

* 225-Lessons Learned This Week
* 224-Employment Privacy & Security


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Trend Micro Anti-Malware Blog

* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

RiskIQ

* Taking a Closer Look at a Malicious Infrastructure Mogul
* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think
* MobileInter: A Popular Magecart Skimmer Redesigned For Your Phone
* DarkSide is Standing Down, But Its Affiliates Live On

FireEye

* What's New in InsightAppSec and tCell: Q2 2021 in Review
* [Security Nation] Brian Honan on creating Ireland's first CERT
* Microsoft SAM File Readability CVE-2021-36934: What You Need to Know
* Grow Your Career at Rapid7: North America Sales
* [The Lost Bots] Episode 1: External Threat Intelligence
* Rapid7 + XDR: Security that Moves as Fast as Your Business
* Rapid7 Acquires IntSights to Tackle the Expanding Threat Landscape
* Accelerating SecOps and Emergent Threat Response with the Insight Platform
* What's New in InsightVM: Q2 2021 in Review
* Metasploit Wrap-Up

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Sage X3 Administration Service Authentication Bypass / Command Execution
* WordPress Backup Guard Authenticated Remote Code Execution
* Sequoia: A Deep Root In Linux's Filesystem Layer
* Ampache 4.4.2 Cross Site Scripting
* CSZ CMS 1.2.9 Arbitrary File Deletion
* News Portal Project 3.1 SQL Injection
* Online Shopping Portal 3.1 SQL Injection
* Vehicle Parking Management System 1.0 SQL Injection
* Vehicle Parking Management System 1.0 Cross Site Scripting
* KevinLAB BEMS 1.0 Authenticated File Path Traversal / Information Disclosure
* KevinLAB BEMS 1.0 Unauthenticated SQL Injection / Authentication Bypass
* KevinLAB BEMS 1.0 Undocumented Backdoor Account
* Dell OpenManage Enterprise Hardcoded Credentails / Privilege Escalation / Deserialization
* Microsoft Windows WFP Default Rules AppContainer Capability Bypass Privilege Escalation
* Webmin 1.973 Cross Site Request Forgery
* WordPress KN Fix Your Title 1.0.1 Cross Site Scripting
* Backdoor.Win32.IRCBot.gen Remote Command Execution
* WordPress Mimetic Books 0.2.13 Cross Site Scripting
* Trojan-Spy.Win32.SpyEyes.hqd Insecure Permissions
* Trojan-Spy.Win32.SpyEyes.abdb Insecure Permissions
* Dolibarr ERP/CRM 10.0.6 Login Brute Forcer
* Backdoor.Win32.Agent.bjev Insecure Permissions
* HEUR.Backdoor.Win32.Winnti.gen Insecure Permissions
* WordPress LearnPress Privilege Escalation
* WordPress LearnPress SQL Injection

CXSecurity

* Sage X3 Administration Service Authentication Bypass / Command Execution
* Dell OpenManage Enterprise Hardcoded Credentails / Privilege Escalation / Deserialization
* Linux Kernel Netfilter Heap Out-Of-Bounds Write
* ForgeRock Access Manager/OpenAM 14.6.3 Remote Code Execution
* Seagate BlackArmor NAS sg2000-2000.1331 Command Injection
* VMware vCenter Server Virtual SAN Health Check Remote Code Execution
* Pandora FMS 7.54 Cross Site Scripting

Proof of Concept (PoC) & Exploits

Exploit Database

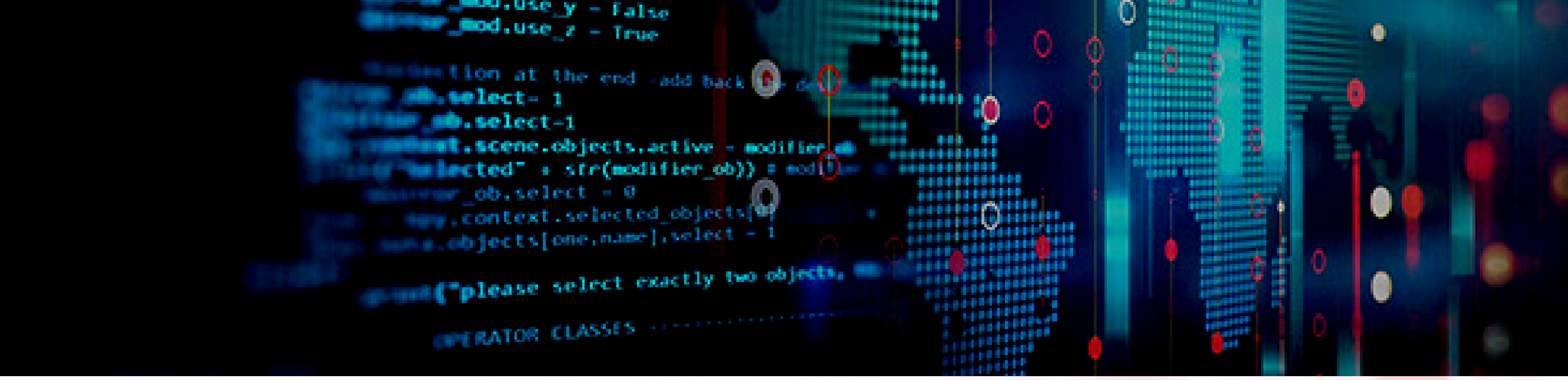
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Arbitrary File Deletion
* [webapps] KevinLAB BEMS 1.0 - File Path Traversal Information Disclosure (Authenticated)
* [webapps] KevinLAB BEMS 1.0 - Unauthenticated SQL Injection / Authentication Bypass
* [remote] KevinLAB BEMS 1.0 - Undocumented Backdoor Account
* [webapps] Webmin 1.973 - 'run.cgi' Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin KN Fix Your Title 1.0.1 - 'Separator' Stored Cross-Site Scripting (XSS)
* [webapps] PEEL Shopping 9.3.0 - 'id' Time-based SQL Injection
* [webapps] Dolibarr ERP/CRM 10.0.6 - Login Brute Force
* [webapps] WordPress Plugin Mimetic Books 0.2.13 - 'Default Publisher ID field' Stored Cross-Site Scri
* [webapps] WordPress Plugin LearnPress 3.2.6.8 - Privilege Escalation
* [webapps] WordPress Plugin LearnPress 3.2.6.7 - 'current_items' SQL Injection (Authenticated)
* [remote] Aruba Instant (IAP) - Remote Code Execution
* [local] Linux Kernel 2.6.19
* [remote] Aruba Instant 8.7.1.0 - Arbitrary File Modification
* [webapps] Seagate BlackArmor NAS sg2000-2000.1331 - Command Injection
* [webapps] ForgeRock Access Manager/OpenAM 14.6.3 - Remote Code Execution (RCE) (Unauthenticated)
* [local] Argus Surveillance DVR 4.0 - Weak Password Encryption
* [webapps] WordPress Plugin Popular Posts 5.3.2 - Remote Code Execution (RCE) (Authenticated)
* [webapps] osCommerce 2.3.4.1 - Remote Code Execution (2)
* [webapps] WordPress Plugin Current Book 1.0.1 - 'Book Title and Author field' Stored Cross-Site Scrip
* [webapps] Webmin 1.973 - 'save_user.cgi' Cross-Site Request Forgery (CSRF)
* [webapps] Garbage Collection Management System 1.0 - SQL Injection + Arbitrary File Upload
* [webapps] OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution (Authenticated) (2)
* [webapps] Invoice System 1.0 - 'Multiple' Stored Cross-Site Scripting (XSS)

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

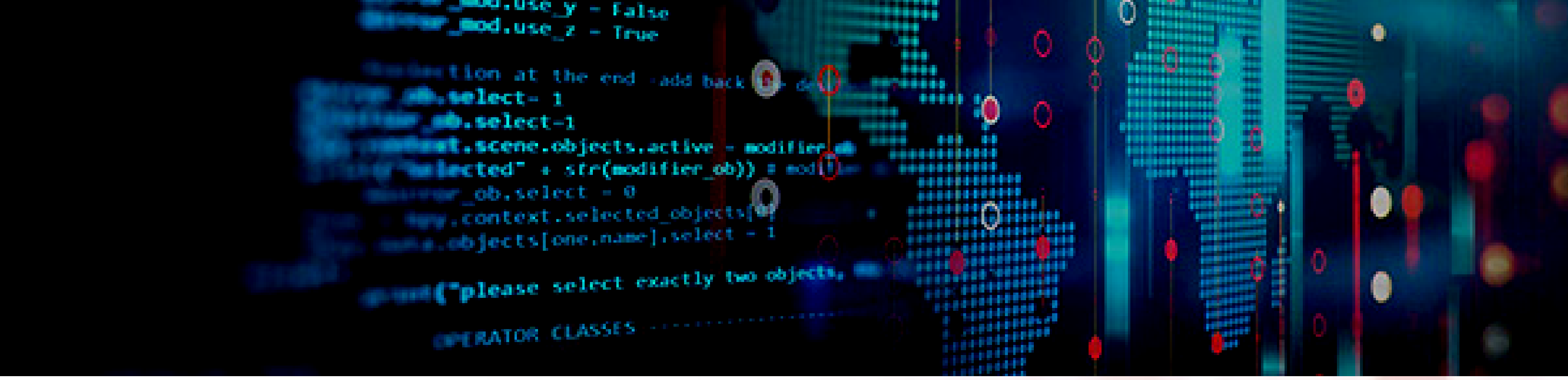
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Latest Hacked Websites

Published on Zone-h.org

Unfortunately, at the time of this report, the Zone-H.org last hacked feed was not availible.


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier
"elected" + str(modifier_ob)) # modif
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects
OPERATOR CLASSES

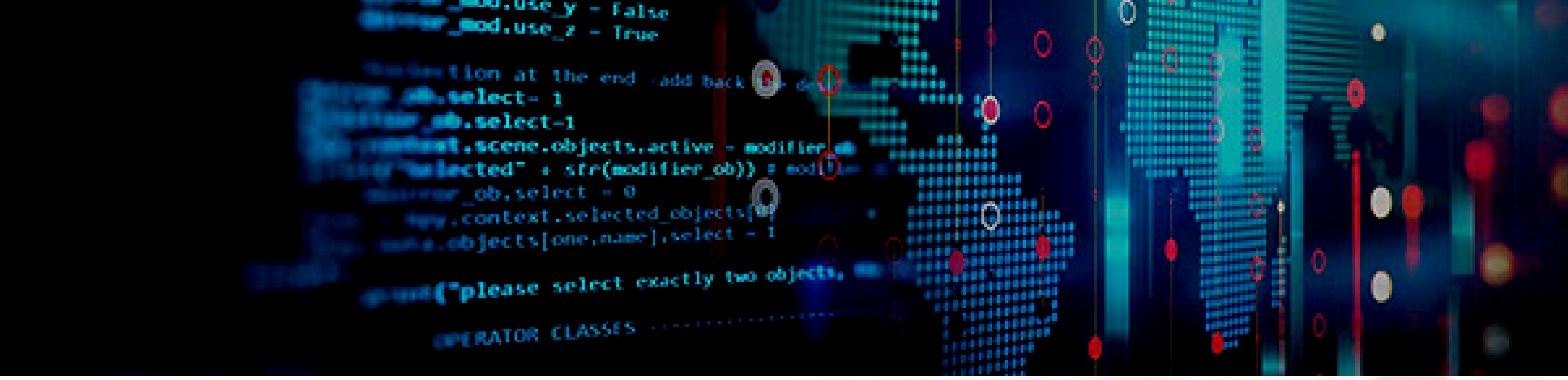
Dark Web News

Darknet Live

[Student Sentenced for Reselling Drugs Sourced on the Darkweb]
A student at the University of Chester was sentenced to prison for buying drugs on the darkweb and selling them locally. (via darknetlive.com)
Dream Vendor "FatSam" Avoids Prison in Drug Case
A judge in the U.K. sentenced a Dream Market vendor to time served and community service instead of time behind bars. (via darknetlive.com)
Operation DisrupTor: Cocaine Vendor Sentenced to Prison
A darkweb vendor has been sentenced to 6.5 years in federal prison for selling more than 4,000 grams of cocaine to customers throughout the United States. (via darknetlive.com)
Reminder: Tor is Ending Support for v2 Onion Services
Tor is depreciating v2 onion services. Soon they will become unreachable and you will feel bad. (via darknetlive.com)

Dark Web Link

The Crypto World Is Getting Greener. Is It Too Little Too Late?
Non-fungible tokens, or NFTs, are red-hot in both the literal and figurative senses, as they are fashionable and contribute to global warming. Environmentalists have slammed blockchain supporters in recent months for bringing a technology into the mainstream that requires a lot of energy, but are they correct? While there is a problem, there is also [...] The post The Crypto World Is Getting Greener. Is It Too Little Too Late? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Crypto Ransom Recovery: All You Need To Know
There was a wave of panic when ransomware hit the Colonial Pipeline earlier this year. It was most likely the first time ransomware had affected millions of people. The company paid the ransom in exchange for a decryption tool that allowed the company's billing system to be restored online within a few hours.However, the process [...] The post Crypto Ransom Recovery: All You Need To Know appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
5 Common Cash App Scams And How To Avoid Them
Cash Tool is being used by thieves and fraudsters to steal cash, rising concerns regarding how safe this contactless payment app can be. Is Cash App secure? As people abandon cash in the aftermath of the Coronavirus, money-transfer apps like Cash App have surged in popularity but scams on these apps are also on the [...] The post 5 Common Cash App Scams And How To Avoid Them appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Advisories

US-Cert Alerts & bulletins

* &#8239;Cisco Releases Security Updates
* Drupal Releases Security Updates
* 2021 CWE Top 25 Most Dangerous Software Weaknesses
* Malware Targeting Pulse Secure Devices
* Adobe Releases Security Updates for Multiple&#8239;Products&#8239;
* Apple Releases Security Updates
* Google Releases Security Updates for Chrome
* Significant Historical Cyber-Intrusion Campaigns Targeting ICS
* AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013
* AA21-200B: Chinese State-Sponsored Cyber Operations: Observed TTPs
* Vulnerability Summary for the Week of July 12, 2021
* Vulnerability Summary for the Week of July 5, 2021

Zero Day Initiative Advisories

ZDI-CAN-14204: Omron
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-07-20, 2 days ago. The vendor is given until 2021-11-17 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-14260: Siemens
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-07-20, 2 days ago. The vendor is given until 2021-11-17 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-14460: Schneider Electric
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-07-20, 2 days ago. The vendor is given until 2021-11-17 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-14119: Avira
A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-19, 3 days ago. The vendor is given until 2021-11-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-14124: Avira
A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-19, 3 days ago. The vendor is given until 2021-11-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-14635: Avira

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-19, 3 days ago. The vendor is given until 2021-11-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13893: Schneider Electric

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-07-15, 7 days ago. The vendor is given until 2021-11-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13882: Trend Micro

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Wojciech Regu\xc5\x82a (@_r3ggi)' was reported to the affected vendor on: 2021-07-15, 7 days ago. The vendor is given until 2021-11-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14203: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14198: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14603: Microsoft

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14267: Esri

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14381: Ecava

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14275: Ecava

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14605: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14280: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14382: Ecava

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14437: Esri

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14385: Apple

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jzhu' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14384: Ecava

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14587: Trend Micro

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14439: Esri

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14473: Esri

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14383: Ecava

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-13, 9 days ago. The vendor is given until 2021-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-2865-01

Red Hat Security Advisory 2021-2865-01 - The ovirt-engine package provides the manager for virtualization environments. This manager enables admins to define hosts and networks, as well as to add storage, create VMs and manage user permissions. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-2736-01

Red Hat Security Advisory 2021-2736-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-2779-01

Red Hat Security Advisory 2021-2779-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for Windows serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2780-01

Red Hat Security Advisory 2021-2780-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2777-01

Red Hat Security Advisory 2021-2777-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2778-01

Red Hat Security Advisory 2021-2778-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Gentoo Linux Security Advisory 202107-50

Gentoo Linux Security Advisory 202107-50 - A vulnerability in Singularity could result in remote code execution. Versions less than 3.7.4 are affected.

Gentoo Linux Security Advisory 202107-49

Gentoo Linux Security Advisory 202107-49 - Multiple vulnerabilities have been found in Chromium and Google Chrome, the worst of which could result in the arbitrary execution of code. Versions less than 91.0.4472.164 are affected.

Ubuntu Security Notice USN-5020-1

Ubuntu Security Notice 5020-1 - It was discovered that Ruby incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. It was discovered that Ruby incorrectly handled certain inputs. An attacker could possibly use this issue to conduct port scans and service banner extractions. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. Various other issues were also addressed.

Red Hat Security Advisory 2021-2737-01

Red Hat Security Advisory 2021-2737-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4336-2

Ubuntu Security Notice 4336-2 - USN-4336-1 fixed several vulnerabilities in GNU binutils. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that GNU binutils contained a large number of security issues. If a user or automated system were tricked into processing a specially-crafted file, a remote attacker could cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2845-01

Red Hat Security Advisory 2021-2845-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.

Red Hat Security Advisory 2021-2774-01

Red Hat Security Advisory 2021-2774-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.

Red Hat Security Advisory 2021-2775-01

Red Hat Security Advisory 2021-2775-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.

Red Hat Security Advisory 2021-2776-01

Red Hat Security Advisory 2021-2776-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit.

Red Hat Security Advisory 2021-2784-01

Red Hat Security Advisory 2021-2784-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2021-2782-01

Red Hat Security Advisory 2021-2782-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2021-2781-01

Red Hat Security Advisory 2021-2781-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2021-2783-01

Red Hat Security Advisory 2021-2783-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Ubuntu Security Notice USN-5019-1

Ubuntu Security Notice 5019-1 - It was discovered that an assert could be triggered in the NVIDIA graphics drivers. A local attacker could use this to cause a denial of service. It was discovered that the NVIDIA graphics drivers permitted an out-of-bounds array access. A local attacker could use this to cause a denial of service or possibly expose sensitive information. Various other issues were also addressed.

Red Hat Security Advisory 2021-2725-01

Red Hat Security Advisory 2021-2725-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include double free and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2726-01

Red Hat Security Advisory 2021-2726-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-2728-01

Red Hat Security Advisory 2021-2728-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-2729-01

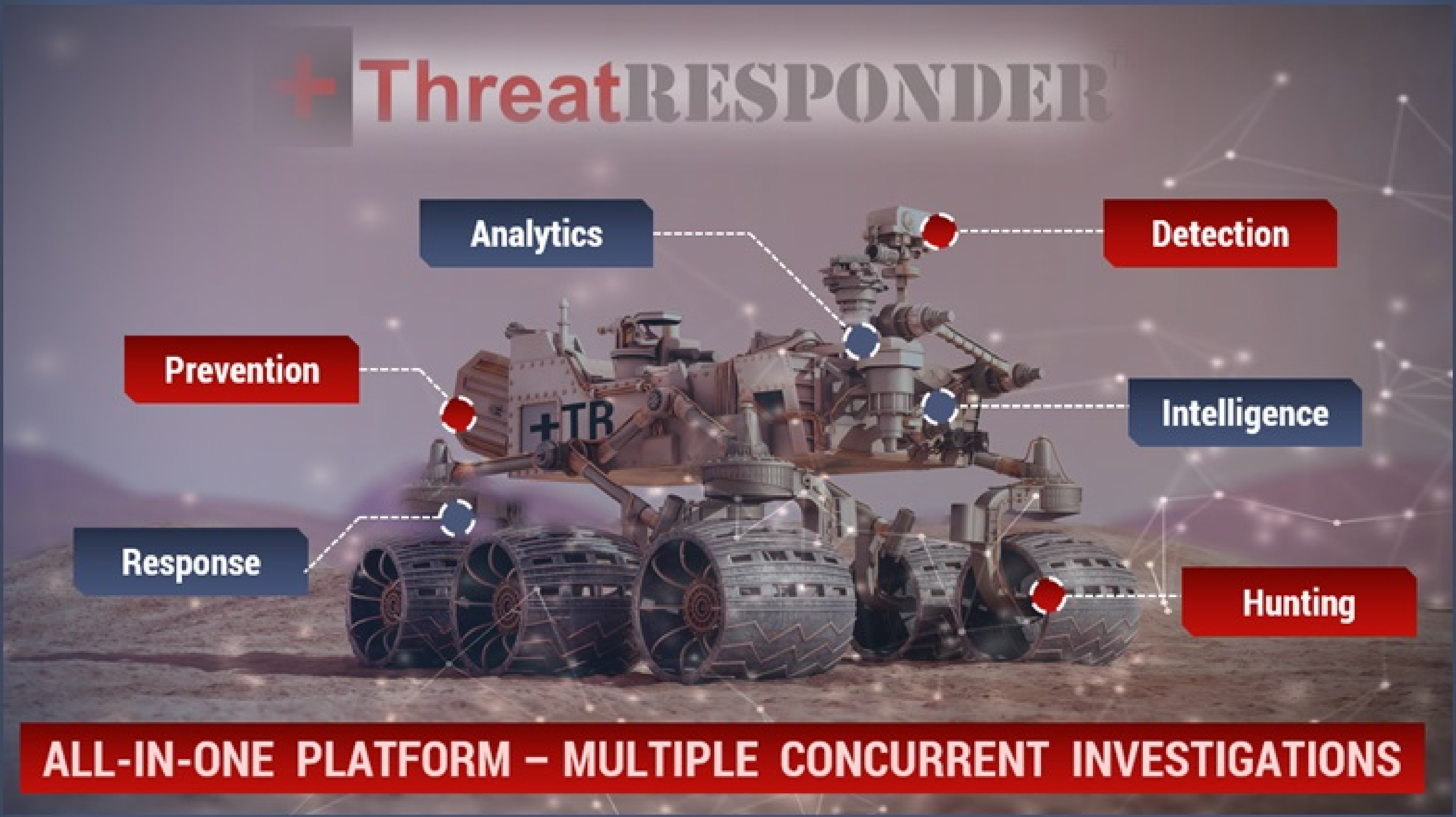
Red Hat Security Advisory 2021-2729-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Are You…

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

CSI Linux is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux has been rebuilt from the ground up on Ubuntu 20.04 LTS to provide long term support for the backend OS and has become a powerful Investigation environment that comes in both the traditional Virtual Machine option and a bootable image that you can install onto an external drive or USB to use as your daily driver or DFIR triage drive. The SIEM has been given an evolution boost with capability while being encapsulated into a Docker container

CSI Linux Tutorials:

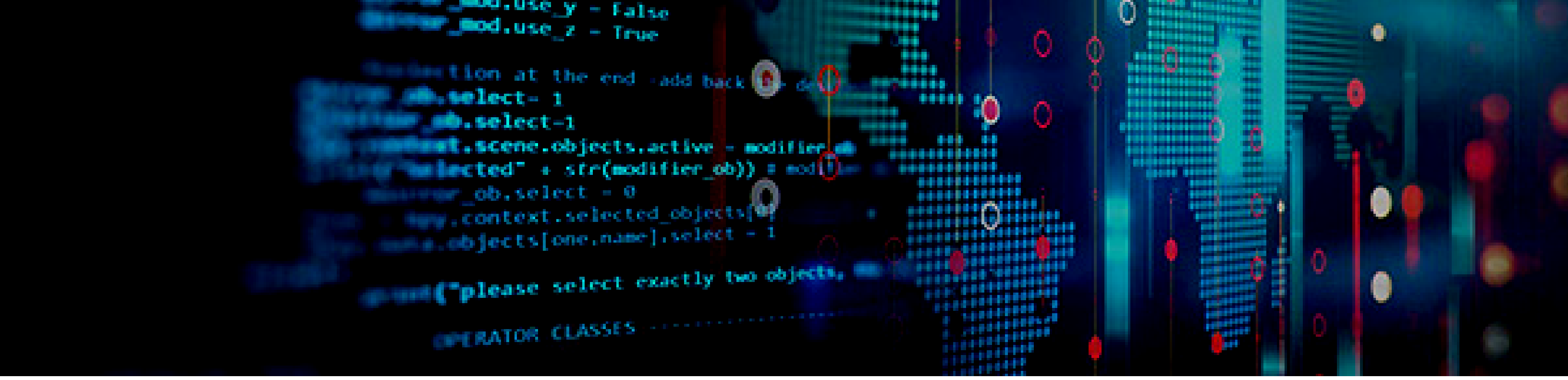
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:
 * Amazon FireTV App - amzn.to/30oiUpE
 * YouTube - youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg

Printed / Kindle Publications:
 * Cyber Secrets on Amazon - amzn.to/2UuIG9B

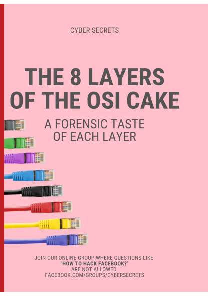


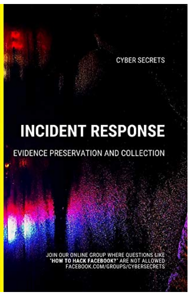
The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

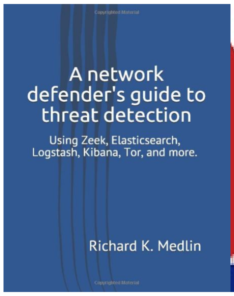
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

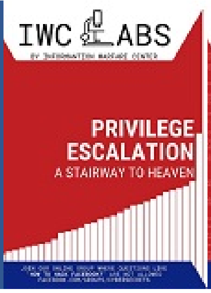
CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel

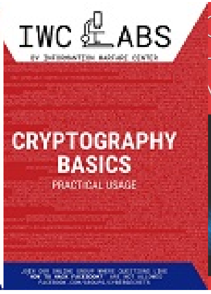


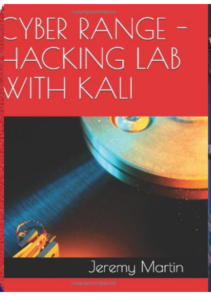


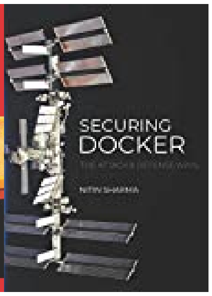
Other Publications from Information Warfare Center











CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP